III. REMARKS

Claims 1, 6, 11 and 24 are amended.

Claims 1, 6, 11 and 24 are patentable under 35 USC 112, first paragraph. The Examiner asserts that the subject matter "the remote network receives the second data without an identity of the predetermined equipment associated with the second data being known to the remote network" is not described in the specification in such a way as to reasonably convey to one skilled in the art that the inventor(s), at the time the application was filed, has possession of the claimed invention. However, this is not the test for enablement under 35 USC 112, first paragraph. The Examiner is reminded that the correct test for enablement under 35 USC 112, first paragraph "is whether one reasonably skilled in the art could make or use the invention from the disclosures in the patent coupled with information known in the art without undue experimentation." *United States v. Telectronics, Inc.*, 857 F.2d 778, 785, 8 USPQ2d 1217, 1223 (Fed. Cir. 1988); see also *In re Wands*, 858 F.2d 731, 737, 8 USPQ2d 1400, 1404 (Fed. Cir. 1988).

It is submitted that one reasonably skilled in the art can make or use the claimed invention without undue experimentation from the disclosure as filed. For example, page 4, lines 22-29 of Applicant's disclosure recites "[d]ata networks trafficking in this sensitive data, such as the internet, may employ commonly available encryption method such as SSL and firewalls, but customers in the rapidly changing semiconductor fabrication industry tend to be extremely reticent to expose data to such data networks unless a scheme can be devised that offers an exceedingly high level of security." As such, it is an object of the present application to provide security for semiconductor fabrication tools. In addition, for exemplary purposes only, page 13, lines 2-18 recites that "the user cannot directly access the tool 102 from the remote control viewer 170 because the user must go through the second network 110" and that "[i]t is a feature of the present invention to allow a user to access a tool from a remote network to prevent direct IP routing to the tool and keep communications secure." Further, for exemplary purposes only, page 14, line 26 through page 15, line 13 describes that all communications between the user of the desktop 200 in the remote network and the tool 102 in the local network are made through the equipment diagnostic monitoring system 120. Thus, because the specification as filed describes that security of the tool is provided by passing all communications trough the equipment diagnostic monitoring system such that direct IP routing to the tool is avoided, it naturally follows that the remote network receives the second data without an identity of the predetermined equipment associated with the second data being known to the remote network. Thus, one reasonably skilled in the art would undoubtedly be able to make or use the claimed invention without undue experimentation based on the specification as filed.

The Examiner appears to be basing the 35 USC 112, first paragraph rejection solely on the language used in the claim not being recited word for word in the specification. However, as described above, this is not the test for enablement under 35 USC 112, first paragraph. It is also noted that the language used in the claims (i.e. the remote network receives the second data without an identity of the predetermined equipment associated with the second data being known to the remote network) is merely paraphrasing what is clearly described in the specification as filed (see the exemplary citations to Applicant's specification noted above). Thus, it is absolutely certain that one reasonably skilled in the art would be able to make or use the invention as claimed from Applicant's specification without undue experimentation. Therefore, the rejection under 35 USC 112, first paragraph is unfounded and should be withdrawn.

Claims 1-36 are patentable under 35 USC 103(a) over the combination of Pyotsia et al. (US 7010294, hereinafter "Pyotsia") and Reid et al. (US 6182226, hereinafter "Reid"). Claim 1 recites the module being configured to monitor the predetermined equipment substantially independent of input from the remote network. This feature is not disclosed or suggested by the combination of Pyotsia and Reid.

In Pyotsia all of the diagnostics are performed "live" by an operator in a control room or by the mobile terminal user. For example each field device type in Pyotsia is provided with a specific control software which contains all necessary data and instruction sets for controlling, configuring, reading, etc., the field devices of a predetermined time. These operations are normally made by a control room personnel from a work station. (Col. 5, L. 19-42). Further, column 8, lines 1-15 of Pyotsia describe an interactive user interface and an "on-line" connection through which maintenance personnel are able to retrieve information on the operation of a desired field device and display it on the user interface of the mobile terminal. The operational data obtained by the mobile terminal allows the maintenance person to immediately made a decision on the maintenance need of the respective field device. There is absolutely no disclosure in Pyotsia of a module being configured to monitor the predetermined equipment substantially independent of input from the remote network as recited in Applicant's claim 1. Combining Pyotsia with Reid fails to remedy this deficiency as Reid is absolutely silent as to this feature of claim 1.

Thus, claim 1 is patentable over the combination of Pyotsia and Reid at least because the combination of Pyotsia and Reid fails to disclose or suggest the module being configured to monitor the predetermined equipment substantially independent of input from the remote network as recited in claim 1. Claims 6, 11 and 24 are patentable over the combination of Pyotsia and Reid for reasons that are substantially similar to those described above with respect to claim 1.

Further, claim 1 recites that the remote network receives the second data without an identity of the predetermined equipment associated with the second data being known to the remote network. The examiner admits that this feature of claim 1 is not disclosed or suggested by Pyotsia. However, the Examiner asserts that this feature of claim 1 is disclosed in Reid at column 6, lines 46-56.

It is noted that column 6, lines 46-56 of Reid merely discloses:

> A rewrite node is a point in an access rule where source or destination addresses are mapped to other source or destination addresses. Destination IP address rewrites allow an inbound connection through network address translation (NAT) address hiding to be remapped to a destination inside the NAT barrier. Source address rewrites can be used on outbound

> connections to make the source appear to be one of many external addresses. This process allows the internal hosts to be aliased to external addresses. Rewrites can be based on any connection criteria, including users.

While Reid describes address hiding and remapping, Reid does not disclose the above noted features of claim 1. Applicant's claim 1 calls for a transfer of data regarding a predetermined condition of predetermined equipment identified by the module, wherein the remote network receives the second data without an identity of the predetermined equipment associated with the second data being known to the remote network. The mere recitation of address hiding and remapping cannot reasonably be considered as disclosing the above noted features of Applicant's claim 1. Thus, claim 1 is patentable over the combination of Pyotsia and Reid.

It is also submitted that Pyotsia and Reid have been combined improperly as Pyotsia expressly teaches against a combination with Reid. Further, modifying Pyotsia with Reid would change the principal of operation of Pyotsia as well as render Pyotsia unsuitable for its intended purpose. It is requested that the Examiner explain why Pyotsia and Reid are combinable despite Pyotsia teaching against such a combination and the fact that such a combination would change the principal of operation of Pyotsia as well as render Pyotsia unsuitable for its intended purpose as described below.

It is submitted that the remote network receives the second data without an identity of the predetermined equipment associated with the second data being known to the remote network is not obvious to one skilled in the art as Pyotsia specifically teaches against destination IP address rewrites as described in Reid. The Examiner is reminded that "[a] prior art reference must be considered in its entirety, i.e., as a whole, including portions that would lead away from the claimed invention." *W.L. Gore & Associates, Inc. v. Garlock, Inc.*, 721 F.2d 1540, 220 USPQ 303 (Fed. Cir. 1983), *cert. denied*, 469 U.S. 851 (1984); MPEP § 2141.02.

In Reid the IP address rewrites are disclosed as allowing "an inbound connection through network address translation (NAT) address hiding to be remapped to a destination address inside the NAT barrier. Source address rewrites can be used on outbound connections to make the source appear to be one of many external addresses. This process allows the internal hosts to be aliased to external addresses."

Contrary to the aliasing of internal hosts to external addresses and address hiding of Reid, Pyotsia requires the identity of the field devices to be known in order for the user to access the field device. Thus, Pyotsia directly teaches against the address hiding and rewriting of Reid. For example, Pyotsia discloses remotely controlling, configuring or monitoring field devices with a general purpose mobile terminal (Col. 3, L. 6-10). In Pyotsia the user knows exactly which field device within the plant is being accessed. For example, referring to column 8, lines 30-65 Pyotsia discloses that the WWW server 23 or 33 is arranged to assist the selection of the desired field device by providing a hierarchic set of WWW pages representing the logical, functional or location architecture of the plant in a tree configuration. In Pytosia the user selects a desired plant 1, 2, 3, 4 from the WWW page shown in FIG. 4A and is then directed to a new WWW page where the user selects an area of the plant as shown in FIG. 4B. After the area of the plant is selected the user is presented with another new WWW page for selecting the desired tag from a list. After the desired tag is selected the user is presented with a WWW page of the desired field device. Pyotsia specifically recites that the tag is a unique code used for identification of each field device in the plant (Col. 8, L. 59-65).

Thus, one skilled in the art would not look to the address hiding and rewrites of Reid for modifying Pyotsia because Pyotsia expressly requires the identity of the field devices to be known in order for the user to select the identity of the field device from the list provided on the WWW page. Therefore, claim 1 is patentable over the combination of Pyotsia and Reid at least for this reason.

Moreover, modifying Pyotsia with Reid would change the principle of operation of Reid. The Examiner is reminded that "[i]f the proposed modification or combination of the prior art would change the principle of operation of the prior art invention being modified, then the teachings of the references are not sufficient to render the claims *prima facie* obvious." *In re Ratti*, 270 F.2d 810, 123 USPQ 349 (CCPA 1959); MPEP § 2143.01.

The Examiner argues that it would have been obvious to one of ordinary skill in the art to replace the WAP security of Pyotsia with the network address translation (NAT) of Reid as a predictable use of a known technique of providing security over the network. However, the WAP used in Pyotsia is to verify that the user is an authorized user not to hide an identity of the user (or an identity of the field devices) (see Pyotsia at Col. 7, L. 25-30). Pyotsia specifically recites at column 7, lines 25-30 that "[t]he security and authentication of the user is especially important when the inventive arrangement is used for configuration and control of the field devices. As configuration and control commands will affect on the operation of the plant, a system according to the invention has to assure that the user is an authorized user." If the NAT of Reid were combined with the WAP of Pyotsia so that the identity of the user is remapped and hidden this would be effectively defeating the purpose of the WAP in Pyotsia which is to provide authentication of the user. Thus, the manner in which the users are authenticated would have to be completely redesigned to accommodate the address hiding and remapping of Reid.

Further, if the NAT of Reid were used in the system of Pyotsia for hiding and remapping the identity of the field devices, the hierarchical set of WWW pages of Pyotsia would be rendered useless as the identity of the field devices (as well as the identity of the plant and the location within the plant) is required to allow a user access to the field devices. If Pyotsia were modified with the NAT of Reid for hiding and remapping an identity of the field devices, the way the field devices are accessed in Pyotsia would have to be completely redesigned for allowing access to the hidden and remapped field devices.

Thus, replacing the WAP security of Pyotsia with the NAT of Reid is not a predictable use of a known technique of providing security over the network as argued by the Examiner. Rather, modifying Pyotsia with Reid would change the principle of operation of Pyotsia to the point where the disclosure provided in Pyotsia is unidentifiable due to the necessary redesigning of virtually the entirety of Pyotsia (which requires the identity of the plant, location within the plant and the field devices to be known by the user) to accommodate the NAT of Reid. The address hiding and remapping of Reid is simply not compatible with the a hierarchical set of WWW pages that explicitly use the identity of the desired plant, then an identity of the desired area of the plant and lastly an identity of the desired field device for allowing a user to access a field device (see Col. 8, L. 59-65). Therefore, claim 1 is patentable over the combination of Pyotsia and Reid for this additional reason.

Modifying Pyotsia with Reid as suggested by the Examiner would also render Pyotsia unsatisfactory for its intended purpose. The Examiner is reminded that "[i]f proposed modification would render the prior art invention being modified unsatisfactory for its intended purpose, then there is no suggestion or motivation to make the proposed modification." *In re Gordon*, 733 F.2d 900, 221 USPQ 1125 (Fed. Cir. 1984); MPEP § 2143.01. As described above, Pyotsia requires the identity of the field devices to be known so they can be presented in the hierarchical set of WWW pages. This hierarchical set of WWW pages allows a user to select a specific field device in a specific location of a specific plant (Col. 8, L. 30-65). The address hiding and remapping of Reid would effectively remove the identity of the field devices, the plant and the location of the field devices within the plant the from these WWW pages leaving the user unable to access a specific field device located in a specific location of s specific plant as the user would no longer know or be able to determine the location of the field devices due to the address hiding and remapping leaving Pyotsia unsatisfactory for its intended purpose. Thus, claim 1 is patentable over the combination of Pyotsia and Reid for this additional reason.

Claim 6 also recites the module is configured to convey test data related to the plurality of equipment, to users on the remote network, without an identity of the plurality of equipment being known to the remote network. Claim 11 recites the remote network receives the second data without an identity of the predetermined equipment associated with the second data being known to the remote network. Claim 24 recites an equipment diagnostic monitor system configured to allow a user of the remote network to remotely control a diagnostic test performed on predetermined equipment for monitoring a health of the predetermined equipment without an identity of the predetermined equipment being known to the user of the remote network. Claims 6, 11 and 24 are patentable over the combination of Pyotsia and Reid for reasons that are substantially similar to those additional reasons described above with respect to claim 1.

In addition, claim 6 calls for the module being configured to allow one of the plurality of users to select at least one equipment diagnostic monitor systems from a plurality of equipment diagnostic monitor systems. This feature is not disclosed or suggested by the combination of Pyotsia and Reid. The Examiner admits that Pyotsia does not disclose a "plurality of equipment diagnostic monitoring systems. Therefore, Pyotsia cannot reasonably be considered as disclosing allowing one of the plurality of users to select at least one equipment diagnostic monitor system as called for in Applicant's claim 6. Despite the failure of Pyotsia to disclose the above noted features of claim 6, the Examiner asserts that one of ordinary skill in the art could have used more than one of Pyotsia's "diagnostic systems" to monitor the devices in various LAN network segments independently and the results of such extension of Pyotsia's invention would have been predictable in that the devices located at different segments of the LANs could be independently remotely controlled and monitored. This assertion appears to be based on nothing more than hindsight, especially given the fact that Pyotsia does not disclose or suggest allowing one of the plurality of users to select at least one equipment diagnostic monitor systems from a plurality of equipment diagnostic monitor systems as described above and as admitted by the Examiner. Reid is absolutely silent as to these features of claim 6. Thus, claim 6 is patentable over the combination of Pyotsia and Reid at least for this additional reason.

Claims 2-5, 7-10, 12-23 and 25-36 depend from claims 1, 6, 11 and 24 and are patentable at least by reason of their respective dependencies.

Further, claim 17 recites the user on the remote network sends a suggestion regarding an operation of the at least one item being monitored to an entity managing the at least one item on the local network. Claim 30 also recites that the local network is configured to receive and display a suggestion from the user on the remote network regarding the operation of the equipment being monitored on the local network. Nowhere are these features of claims 17 and 30 disclosed or suggested by the combination of Pyotsia and Reid. The Examiner refers to column 6, line 63 through column 7, line 67 of Pyotsia as disclosing this feature, however all that this cited portion of Pyotsia discloses is the translation of data from one protocol to another and the creation of interactive WWW pages and nothing more. All that is disclosed in Pyotsia is the control of a field device through an interactive WWW page displayed on the mobile terminal. There is no disclosure anywhere in Pyotsia "that the local network is configured to receive and display a suggestion from the user on the remote network regarding the operation of the equipment being monitored on the local network" as recited in claims 17 and 30. Thus, claims 17 and 30 are patentable for this additional reason.

Claims 20-23, 35, and 36 are patentable under 35 U.S.C. 103(a) over Pyotsia and Crist et al., U.S. Patent No. 6,879,940 ("Crist"). It is noted that the Examiner refers to Crist as being US Patent No. 6182226, which is incorrect as this is the Patent number for Reid. This error makes the office action unclear as to which patent the Examiner is referring to with respect to Crist and is grounds for issuance of a corrected office action. However, in the interest of expediting prosecution, Applicant is assuming the Crist reference to be US Patent No. 6879940.

Claims 20-23 and 36 depend from claim 11 and claim 35 depends from claim 1. It is submitted that because the combination of Pyotsia and Reid fails to disclose or suggest all the features of claims 1 and 11 that the combination of Pyotsia, Reid and Crist cannot as well. Therefore, claims 20-23, 35, and 36 are patentable at least by reason of their respective dependencies.

Further, claim 21 recites that the intermediate network further comprises an equipment diagnostic monitor system that monitors and analyses the semiconductor tool. The Examiner argues that it would have been obvious to apply the system of Pyotsia to the testing of a semiconductor tool coupled to the local network, as the application promises the predictable results as stated by Pyotsia at col. 6, line 63 - col. 7, line 67. This statement by the Examiner amounts to nothing more than a conclusory statement. The Examiner is reminded that "rejections on obviousness cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness." *KSR*, 82 USPQ2d at 1396 quoting *In re Kahn*, 441 F.3d 977, 988, 78 USPQ2d 1329, 1336 (Fed. Cir. 2006); MPEP § 2143.01. There is absolutely no reasoning provided by the Examiner. The Examiner merely cites several paragraphs of Pyotsia that describe communication between the mobile terminal MT and the diagnostic system 21 and the information provided to the mobile terminal. The mere recitation of a semiconductor test system (which tests the semiconductors themselves and not the tools used in manufacturing the semiconductors) in Christ does not make it obvious to one skilled in the art to use the system of Pyotsia for testing semiconductor tools especially when there is absolutely no disclosure whatsoever in Pyotsia, Reid and Crist of testing a semiconductor tool as called for in claim 21. Thus, claim 21 is patentable. This argument applies equally to claim 35.

For all of the foregoing reasons, it is respectfully submitted that all of the claims now present in the application are clearly novel and patentable over the prior art of record, and are in proper form for allowance. Accordingly, favorable reconsideration and allowance is respectfully requested. Should any unresolved issues remain, the Examiner is invited to call Applicants' attorney at the telephone number indicated below.

The Commissioner is hereby authorized to charge payment for any fees associated with this communication or credit any over payment to Deposit Account No. 16-1350.

Respectfully submitted,

William J. Knotts, Jr.
Reg. No. 53,145

January 5, 2010
Date

Perman & Green, LLP
99 Hawley Lane
Stratford, CT 06614
(203) 259-1800
Customer No.: 2512